3

Implications for Law Enforcement of the Move to a Cashless Society

GLENN WAHLERT

> *Driven by computer chip technology, possible alternatives to conventional currency are now emerging . . . They raise important issues . . . including the integrity of the issuer, the security and efficiency of the technology, [and] their scope for laundering money* (Bernie Fraser, Governor of the Reserve Bank of Australia).

The emerging technologies associated with stored value and smart cards, digital cash and electronic commerce will clearly pose an unprecedented challenge to regulators generally, and law enforcement specifically, over the next decade.

The powerfully beneficial technologies of telecommunications and computing, which have become the indispensable infrastructure for international commerce, also support the trans-national activities of a variety of criminal enterprises. Around the world organised crime is making use of its vast financial resources and a sophisticated command of technology to move huge amounts of money across continents in seconds.

One concern of the international law enforcement community, is that the convergence of technology, such as the linkage of computers by data transmission and the development of powerful encryption devices, may create new opportunities for criminal groups. To quote a paragraph from a recent study by the International Institute for Strategic Studies at Oxford University:

> *As modern society becomes more dependent on sophisticated communications and information systems, the possibility that these systems will be compromised or disrupted becomes more salient. Transnational criminal organisations can develop the capability to inflict damage [on these systems] relatively easily* (The International Institute for Strategic Studies 1995).

The convergence of communications and information systems is enabling a rapid move to electronic commerce and the empowerment of the individual to have an unprecedented level of control over his or her own money. In many ways this is a positive development, but it does not come without its risks.

Cyberpayments[1] are emerging as an innovative mechanism for conducting financial transactions. These types of transactions, occurring either through the Internet or use of so-called "smart cards", provide a convenient, immediate, relatively secure and anonymous method of transferring financial value.

Cyberpayment systems, albeit in a "first generation" form, currently exist in a

---

1 Cyberpayments: Financial payments and transfers of monetary value conducted either over the Internet and/or through the use of so-called "smart cards".

surprising number of countries (*see* Table 1). With an ever-growing number of people who have access to the Internet, and the ever-increasing number of large banks forging relations with cyberpayments companies, the use of electronic payments is expected to continue to proliferate significantly both domestically and internationally.

Table 1
Countries with Cyberpayment Systems

Europe	North and South America	Asia
England	United States	Hong Kong
Scotland	Canada	China
Denmark	Colombia	Japan
France	Argentina	Singapore
Portugal	Brazil	Taiwan
Belgium	Mexico	Indonesia
Spain		Macao
Finland	**Africa**	Phillippines
Netherlands	Zambia	Sri Lanka
Russia	South Africa	India
Bulgaria		
Germany	**Australia**	

It is not the intention of this paper to show law enforcement as either alarmists or techno-Luddites, but rather to:

- convey a broad overview of some of law enforcements', and other regulators', concerns regarding these unique technologies; and
- examine some of the emerging primary regulatory issues which will directly impact on law enforcement efforts.

Law Enforcement Concerns

Electronic money (or E-cash, DigiCash, CyberCash, and so on) can be used over networks, such as the Internet. Indeed, this is an important driving force behind developments in the technology. Real time E-cash closely emulates paper money, provides person to person payments, may have no audit trail and no interchange.

Essentially E-cash is software which can be programmed to perform specific functions, such as being earmarked for special purposes with conditions on where it can be spent. It can also be transmitted in digital form along computer networks or held in smart cards. In many ways E-cash is more suited to the world of electronic commerce than conventional cash—it is "the ultimate—and inevitable—medium of exchange for an increasingly wired world."

Electronic currencies are not the product of some futurist's imagination; they are very much here and now. The concept of E-cash is best exemplified by the joint National Westminster Bank (NatWest), Midland Bank and British Telecom venture known simply as Mondex. The Mondex electronic money approach closely parallels cash and aims to become a new type of money. Besides Mondex, there are several other companies developing their own form of E-cash.

All these systems are in their infancy, however, and there are no guarantees that they will meet with market acceptance. Nevertheless, a number of E-cash vendors are confident that their products will eventually displace cash as the principal method of payment. For example, Mondex expects E-cash "to account for about a quarter of transactions that take place in society" within ten years. DigiCash, sees electronic money being "pervasive" by 2005, with a number of respected bankers predicting that it will "take off fairly dramatically" within the next five years.

If the amount of interest shown by some large corporations in cyberpayments is anything to go by, digital cash is on its way. In smart card form it is already ubiquitous.

The specific concerns of law enforcement regarding electronic cash can be categorised under the following headings:

- the transportation of illicit funds,
- an inability to trace money flows,
- counterfeiting, and
- non-bank entities as issuers.

Movement of Funds

The physical transportation of cash is often the beginning of the money laundering process. To avoid regulatory and control efforts, particularly in Financial Action Task Force (FATF) member states, money launderers are increasingly simply transporting their funds to a foreign country that has no currency controls and preferably has bank secrecy laws. Once in one of these offshore tax havens, the money can be deposited in a bank or other financial institution and then moved at will.

One of the biggest advantages to criminals from the growth of E-money, will be the simplicity and convenience of transferring value. Once money is converted into a digital form, it can flow in and out of countries at lightning speed using smart card technology, computer networks and, theoretically, other communications devices. Digital cash is ideally suited for international money transfers and, aided by computer software, could be routed and re-routed to several destinations internationally within seconds.

A particular law enforcement concern regarding the enhanced ability to move funds, is the peer-to-peer payment facility being offered by some schemes. At least one card vendor, and several E-cash schemes, plan to offer consumers the ability to anonymously transfer purchasing power from one electronic purse to another; such payment transactions would eliminate the need for clearing procedures and may provide no audit trail, providing opportunities for criminal abuse.

Our concern here is that some of these payment methods are "too close to cash for comfort." While many of the above characteristics are shared with cash, the risks could be magnified when the medium is a single card rather than a wallet full of notes.

Traceability

Another concern relates to the ability of financial transactions and monetary value transfers to "escape" from the regulated banking industry where we, and other regulators, have some level of visibility. E-money may be easily sent in and out of a country undetected, facilitating money laundering on a grand scale and weakening a national government's ability to monitor transactions and tax. A number of the electronic money schemes either under development or currently being trialed operate in an environment "where identities are concealed, national borders do not exist and transactions are instantaneous and potentially untraceable."

Imagine a scenario where E-cash is ubiquitous, having largely replaced conventional currency for small value transactions, and is seen as a major competitor for larger value transactions along with credit and debit card purchases. Using advanced smart cards, or computer networks, there would be little need for the funds to re-enter the banking network: they could conceivably move from consumer to consumer, consumer to point of sale, or point of sale to point of sale, just as cash does now.

Criminals could even demand payment in electronic form using electronic purses or the next generation of the electronic purse, the "wallet PC". For example, if drug dealers were able to obtain payment at street level in E-cash, they would have no need for a domestic bank—their funds could be automatically and anonymously deposited in an offshore account without any reference to an Australian bank or clearing house. Alternatively, their E-cash could be simply retained on the card and physically transported out of the country.

Additionally, should the Reserve Bank lose control of even a portion of the money supply through pervasive electronic cash systems, then this could place Australia's current transaction reporting regime in

jeopardy. The Financial Transaction Reports Act relies on the ability of the banks to identify suspicious transactions as well as those over certain predetermined limits.

A report commissioned by Visa International on a number of electronic purse systems, concluded that electronic money, when combined with smart card technology

> *could be used to smuggle currency in and out of countries in violation of those [country's] laws. It can also be used to transact normal business without the knowledge of the authorities, which could make it very useful to the "underground economy"* (Mondex in Comparative Perspective 1994, p. 15).

In some ways this situation is an acknowledgment that "banking is essential to the modern economy, but banks are not."

An example of the challenge facing regulators in attempting to maintain some degree of oversight of financial transactions, is the operation of the World Trade Clearinghouse Ltd's offer of a gold-backed cybercurrency with cash-like anonymity and "protection from bureaucratic snoops, nasty ex-spouses, and lawsuit-hungry lawyers." Similarly, the Internet Online Offshore Casino, run out of the Turks and Caicos Islands in the Bahamas, promises to accept all manner of E-money and pay interest on balances they leave in an offshore bank the company recently bought.

Counterfeiting

Besides the possibilities of E-cash presenting opportunities for money laundering, some forms of electronic money may prove susceptible to reverse engineering and counterfeiting. If computer hackers or other criminals were to break into E-cash systems they could instantaneously filch the electronic wealth of numerous innocent consumers. Should they also crack the encryption devices guarding such systems, as recently occurred in France, the successful hacker may be able to literally "print" his own money.

The vulnerabilities of these systems to compromise, interception or electronic counterfeiting depends to a large extent on the integrity of the encryption algorithms used, and these are yet to be tested in the market place. Certainly there is some suspicion and, perhaps, healthy scepticism among information technologists to the various advertising promises of total and absolute security.

Another issue to consider, and this is accepted as a potential problem by Wells Fargo in their Mondex trial, is that if these systems are "cracked", forgery may prove extremely hard to detect. It is not as simple as holding up a fifty-dollar note to the light: there are no metallic strips, no holograms, no note texture to feel. If you hold the encryption keys, or copies, you own the mint. A recent report by the Economic Crime Branch of the Royal Canadian Mounted Police, confirms this assessment. In an article entitled "The Future Threat of Credit Card Crime", the author states:

> *In a technological society, these types of crimes are less likely to be detected when one considers the ease at which information, and in particular data, can be transmitted across international boundaries* (Duncan 1995).

From a law enforcement perspective, we will have to assume that digital money will be the subject of sustained attack from all kinds of people.

Unregulated Institutions as Issuers

Both Visa and MasterCard's plans for their electronic purses will maintain the integrity of the Australian Transactions Reports and Analysis Centre (AUSTRAC) reporting regime by ensuring the centrality of the banks in the transaction loop. However, organisations other than banks might also want to issue electronic purses.

A number of the so-called loyalty cards, for example, might look at expanding the functionality of their cards in the future to incorporate "purse", or even "wallet" technology. This is not an unrealistic scenario. Worldwide, telecommunications and transit authorities have taken the lead in developing and employing stored value card (SVC) technology. Additionally, the same players that are looking to deliver information, entertainment and communications services to the home are also interested in payments as an integral part of the package.

The danger here is that as E-cash becomes pervasive and a variety of companies successfully offer their own brand of digital cash, the banks may be bypassed as the primary providers of consumer financial services. The various non-bank purveyors of E-cash, which may include insurance companies, telecommunications carriers and software manufacturers, may become the consumer's first point of contact when they want to obtain some digital money. Combine this possibility with the scenario described above and you would have a need for some very creative work on the part of AUSTRAC to keep ahead of money launderers.

The issue of non-bank involvement in the provision of electronic purse services was explored by European Economic Community policymakers. A May 1994 report from the working group on European payment systems proposed that only banks be allowed to issue electronic purses. The report cautions that cards issued by nonbanks would not be subject to the banking regulations, supervision and deposit insurance schemes that have traditionally protected consumers. Similarly, this level of regulation and supervision has also provided a bulwark against money laundering.

At the November 1994 Financial Action Task Force (FATF) meeting in Paris, it was noted that laundering operations were spreading outwards from the banking to non-banking sector as launderers become more aware of the various directives, legislation and conventions requiring banks and financial institutions to follow the standard requirements of identification and reporting. These non-bank institutions, ranging from large to small less-traditional financial intermediaries, are subject to fewer regulatory requirements and examinations, making them potentially more vulnerable to money laundering.

Is Regulation the Answer?

The concept of electronic money raises a number of questions that are, as yet, unanswered: Who should be allowed to issue E-cash, and who will regulate the issuers? How will taxes be applied in cyberspace, which transcends physical boundaries? How will regulators police money laundering and counterfeiting on private networks? There are a number of aspects to these issues.

Firstly, we must acknowledge that existing monetary regulations do not cover all of the potential uses of E-cash. These systems present untold, and yet to be understood, opportunities for launderers. They are also entirely outside of the current legislative and regulatory regime in Australia, and the regulatory gaps are sizeable. For example, there are no laws that limit the balance of electronic currency that can be loaded onto a smart card and, if E-cash can transcend international borders, it would not be affected by present international currency exchange efforts.

So is regulation an answer? One aim of regulation is to resolve an issue. In this case it is very difficult to resort to pre-emptive regulation as a resolution of issues we have not as yet identified. It is also too early to make any judgments about the extent to which any of these systems really differ in kind from our present day payment system. We are, therefore, uncertain how our extant regulatory, legal, economic and policy frameworks may be able to evolve to cope with these new products—remembering that these

frameworks were designed to accommodate new developments and have done so successfully so far: for example, credit/debit cards, EFTPOS, ATMs, and so on. The fundamental question we are unable to answer at this point is to what extent these systems are category killers (that is, developments that do not fit neatly within the existing structure).

Another issue relates to the ability of the regulators generally, and law enforcement specifically, to enforce any state or federal legislation relating to E-cash. It is quite possible that electronic money will prove as hard to regulate as any other form of digital information, especially where it is used on computer networks or transferred over other communications devices. The anarchical structure of the Internet and the almost total inability of governments to police pornography and stormfronts on the Net, suggests some of the challenges likely to confront law enforcement within the next ten years. For example, how will governments monitor or control stateless E-money? Questions such as this have special significance for financial crime investigators and organisations such as AUSTRAC and the Australian Taxation Office.

The Law Enforcement Dilemma

Law enforcement faces a difficult dilemma. On the one hand we have an opportunity to influence the development of these schemes: as many are "works in progress" their final shape may ultimately depend on regulatory decisions, or the threat of them. However, these very decisions require information about the systems' projected characteristics that we do not possess. Essentially our dilemma is the same as it is for government: how do we ensure and encourage innovation while addressing issues required by the public interest?

Privacy Issues

Privacy is a related but, arguably, more controversial issue. Some believe that cyberpayments should be, in principle, just as anonymous as cash transactions and view statements such as this a real worry. This creates a dichotomy between privacy and traceability and places many of us, especially law enforcement, at odds with the privacy groups. I would contend that cash is not as anonymous as many of these cyberpayment systems. With cash you are normally required to conduct a face-to-face transaction. This is in some ways traceable. And you cannot shove fifty-dollar notes down the telephone line or into your computer and conduct business. The increased functionality of these new means of payment compounds many of the risks associated with abuse. I am not sure the privacy advocates appreciate this fact fully.

Nevertheless, the political clout of these groups cannot be ignored. It is a relatively simple and attractive proposition for politicians to take the moral high ground and declare their intentions to protect the privacy of consumers. It is far more difficult to promise to maintain the integrity of the systems themselves and protect the consumer from their misuse.

Another issue is the relative importance of privacy to the average consumer. Sure, if you ask them whether they are concerned about the prospect of government and big business being able to keep track of their financial transactions, they will probably answer an emphatic "yes!" But if you then ask them if they are prepared to pay a premium for that privacy you may detect some equivocation.

Privacy advocates may counter this argument by stating that cost is not at issue. However, the aim of my logic is to show that when it comes to the essential drivers of the consumer's decision to use a new product, privacy is not high on his list of priorities. His main concerns are the three Cs: cost, convenience, and confidence. The amazing growth of loyalty schemes suggests that consumers are

willing to trade privacy for some benefit—convenience, cost, or a perk of some sort. Notwithstanding this line of argument, I suspect the privacy groups will maintain a higher profile in the corridors of power than law enforcement. Consequently the trick for me will be to find some middle ground between the demands of privacy and consumer groups on the one hand, and the requirements of law enforcement for a more transparent form of currency on the other. It is also important to keep emphasising that privacy and anonymity are not synonymous.

What can be Done?

First of all we need to understand these emerging systems a lot better than we do today. Secondly, law enforcement and regulatory communities will need to work closely with financial institutions, and other entities which are providing cyberpayment services, in identifying, addressing, and possibly resolving emerging issues and areas of potential mutual concern. In particular, we need to develop viable guidelines for pursuing know your customer policies and suspicious transaction detection strategies.

Concurrently we must foster international cooperation among law enforcement, regulatory, and industry representatives to address the possible erosion of international financial borders, and develop strategies for ensuring the integrity and viability of these systems.

Conclusion

Rapidly advancing technology is stimulating an inexorable international move towards electronic commerce and the growth of electronic forms of payment. The next year or two will likely witness the introduction of a complementary instrument, an electronic analogue to cash known as the electronic purse. Although we cannot predict how rapidly and widely this new technology will be accepted and just what forms it will assume, dramatic changes are clearly possible over the next several years both in the way consumers make payments and how they view money. Additionally, many of the existing forms of electronic payment, such as EFTPOS and credit-cards, are likely to continue to replace coins and notes ensuring that paper money at least withers, if not dies. While Australia may not be destined to become a "cashless" economy for some time, it is certainly credible that the relentless advance of electronic payments will make us one with "less-cash".

In the first decade of next century, consumers will be increasingly able to shop from home, gamble remotely and transfer funds without visiting a financial institution. As society moves towards fewer and fewer face-to-face financial transactions there is a possibility that this will present law enforcement with a number of challenges. Principal among these challenges may be the increasingly anonymous nature of crime and the further internationalisation and sophistication of criminal activity utilising powerful encryption devices and computer networks.

Allow me to leave you with one final thought:

> *Crime knows no frontiers [especially in cyberspace], but law enforcement does.*

References

Duncan, M.G.D. (Economic Crime Branch, Royal Canadian Mounted Police HQ) 1995, "The future threat of credit card fraud", *RCMP Gazette*, vol. 57, October, pp. 25-6.

Mondex in Comparative Perspective 1994, Report Commissioned by Visa International.

The International Institute for Strategic Studies 1995, *Strategic Survey 1994-95*, Oxford University Press, Oxford.